Privacy Impact Assessment (PIA)
for the

Enterprise Identity, Credential, and Access Management (ICAM)
June 16, 2020

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Michel Gray, Project Manager
Contact Email: michael.gray@ed.gov

System Owner

Name/Title: Roman Kulbashny, Branch Chief
Principal Office: Office of the Chief Information Officer (OCIO)

Please submit completed Privacy Impact Assessments to the Privacy Office at
privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, please answer with N/A.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The Enterprise ICAM system will be a Department-wide identity, credential, and access management solution based on the Oracle Identity Management suite of products. The solution will provide a robust platform that enables the management of identity data, credentials, identity lifecycle management processes as well as provides authentication and authorization services to various Department systems. The Enterprise ICAM system is a new system and will be the central repository and authoritative source for identity management across the Department, allowing leadership to monitor and manage access to the Department facilities and information systems.

ICAM's development is multi-phased and will require a review and update to this PIA with each new release. This PIA will specifically address the ICAM Phase I Identity Foundation whose purpose will be to provide an authoritative identity directory for all Department employees and contractors. This phase will not include PII of term employees of less than 30 calendar days with monitored access to the Department's information systems.

1.2. Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained or shared.

The system maintains PII of Department employees and contractors to provide an authoritative identity directory of those with electronic access to the Department's network, systems, and information resources.

1.3. Is this a new system, or one that is currently in operation?

New System

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

1.4. Is this PIA new, or is it updating a previous version?

New PIA

1.5. Is the system operated by the agency or by a contractor?

Contractor

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☐ N/A

Yes

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

The Enterprise ICAM system is authorized under the following authorities:

- OMB M-19-17 Enabling Mission Delivery through Improved Identity, Credential, and Access Management
- Homeland Security Presidential Directive 12 (HSPD-12): Policies for a Common Identification Standard for Federal Employees and Contractors
- 5 CFR 731 – Office of Personnel Management, Civil Service Regulations, Suitability
- 5 CFR 732 – Office of Personnel Management, Civil Service Regulations, National Security Positions
- 5 CFR 736 – Office of Personnel Management, Civil Service Regulations, Personnel Investigations
- Executive Order 9397 – Numbering System for Federal Accounts Relating to Individual Persons
- Executive Order 10450 – Security Requirements for Government Employment

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

The PII used in this initial phase of ICAM is currently covered by the EDSTAR SORN.

EDSTAR (18-05-17) published in the Federal Register on November 27, 2007 at 72 FR 66158.
https://www.federalregister.gov/documents/2007/11/27/E7-23059/privacy-act-of-1974-system-of-records-investigatory-material-compiled-for-personnel-security

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

Click here to enter text.

Records Management
If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

General Records Schedule 3.2, Item 030 (DAA-GRS-2013-0006-0003) and Item 031 (DAA-GRS-2013-0006-0004). Disposition instructions: For systems not requiring special accountability for access, records are destroyed when business use ceases. For

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

systems requiring special accountability for access, records are 6 years after user account is terminated, but longer retention is authorized if required for business use.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

The ICAM system will maintain the following information on Department employees and contractors:

- Name, work email, work phone number, work address.
- Organizational data such as supervisor name, address, principal office component (POC), position/title, chain of command, group membership(s).
- System access data such as user access and permission rights, and level of national security clearance.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

The PII in ICAM is obtained from the Department's electronic directory services. When an employee onboards the Department creates an email address based on the employee's first and last name. The additional organizational data is provided by the Department.

In future phases of ICAM, PII will still initially be collected from the Department's electronic directory but will also be sourced from other Department information technology (IT) systems such as Education Security Tracking and Reporting System (EDSTAR), from officials of the Department such as Contracting Officer Representatives, and directly from the individuals themselves.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

The ICAM system obtains PII from the Department's directory service electronically.

In future phases with more sources indicated above in 3.3, ICAM will obtain PII using manual data entry, flat files, database queries, application programming interfaces, vendor-provided or contractor-developed direct connectors, and other web services.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

The Enterprise ICAM system relies on the Department's current electronic directory services for the validity and integrity of the personally identifiable information. In Phase I the Enterprise ICAM system will have a continuous feed of the directory data and it will be able to query for any updates to the data.

In future phases, ICAM will be relied on as the authoritative source for identity management and will validate PII by integrating with other IT systems and Department processes throughout the identity lifecycle.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

PII is used as part of the lifecycle management of an employee or contractor's digital identity to automate the onboarding and offboarding of Department employees and contractors and verify that persons using Department information systems and resources are authorized to do so.

In future phases, PII will be used to link user accounts and credentials to their human owners enabling the Department to ensure that its employees and contractors have the access and privileges they need to perform their official duties. Using this approach, the Department will enter PII into ICAM once, protect it centrally and distribute it to vetted partnering systems in a protected manner thus enhancing control of and access to PII used by Department systems.

[3] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

☑ N/A

Click here to enter text.

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

No

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☑ N/A

Click here to enter text.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☑ N/A

Click here to enter text.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

The Enterprise ICAM system provides public notice via the publishing of a Privacy Impact Assessment.

In future phases, as ICAM integrates with other IT systems and Department processes, the Privacy notices associated with those collections will be updated to indicate internal sharing with ICAM. Additionally, a System of Records Notice for future capabilities of ICAM will be published in the Federal Register.

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☑ N/A

www.ed.gov/privacy

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

The Department's use of ICAM is for the purposes of identity lifecycle management, opting out or declining to provide PII to ICAM will result in an employee or contractor being unable to gain access to the Department's network. For that reason, there are no opportunities for employees and contractors to consent to uses, decline to provide information, or opt out.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

No

5.2. What PII will be shared and with whom?

☑ N/A

Click here to enter text.

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

☑ N/A

In future phases, ICAM will share PII internally with other offices for the purposes of authentication and authorization to Department IT systems.

External

5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

No

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

Click here to enter text.

5.6. What is the purpose for sharing the PII with the specified external entities?

☑ N/A

Click here to enter text.

5.7. Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☑ N/A

Click here to select.

5.9. How is the PII shared with the external entity (e.g. email, computer match, encrypted line, etc.)?

☑ N/A

Click here to enter text.

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☑ N/A

Click here to select.

5.11. Does the project place limitation on re-disclosure?

☑ N/A

Click here to select.

6. Redress

6.1. What are the procedures that allow individuals to access their own information?

If an individual wishes to access their records in ICAM they may reach out directly to the ICAM system owner. Additionally, because the records in the first phase of ICAM are covered by the EDSTAR SORN, individuals may also contact the system manager listed there.

6.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

If an individual wishes to correct inaccurate or erroneous records in ICAM they may reach out directly to the ICAM system owner. Additionally, because the records in the first phase of ICAM are covered by the EDSTAR SORN, individuals may also contact the system manager listed there.

6.3. How does the project notify individuals about the procedures for correcting their information?

Users are notified of these procedures through the publication of this PIA.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Moderate

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

Access to the Enterprise ICAM system is available only to users who have been authenticated to the Department of Education network using their Department issued PIV card. Access to all privileged roles is controlled through processes that enforce formal requests and approvals for access on a need to know and least privilege basis. Enhancing this model, strict separation of duties are in place as well with regards to the distribution of roles. Access to data is protected through physical access controls to the hosting facilities, firewalls, network and host intrusion detection systems, event monitoring systems, nightly backups, and data encryption while at rest and in transit. Additionally, there are scheduled system audits, user recertification and vulnerability scans. Finally, all privileged users are provided a copy of the Rules of Behavior and are required to complete the annual Cybersecurity and Privacy Awareness training.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

No

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

The Enterprise ICAM team at the Department of Education participates in the following continuous monitoring activities to safeguard the Enterprise ICAM system and the PII

information that it manages: vulnerability scans performed at least monthly, annual testing of the Enterprise ICAM Contingency Plan, annual self-assessments and security assessments conducted in conjunction with the security authorization team, and annual updates to the system's security documentation.

The Enterprise ICAM System is hosted within a Department authorized and FedRAMP compliant facility. Therefore, many of the safeguards in place to protect the system are covered by both Departmental and FedRAMP requirements. One of the components for maintaining a security authorization that meets both the Departmental and FedRAMP requirements is continuous monitoring of security controls as a part of the overall risk management framework. Performing ongoing security assessments determines whether the set of deployed security controls in a cloud information system remains effective in light of new exploits and attacks, and planned and unplanned changes that occur in the system and its environment over time. To maintain an authorization that meets the FedRAMP requirements, the cloud service provider must monitor their security controls, assess them on a regular basis, and demonstrate that the security posture of their service offering is continuously acceptable. Security control assessments performed periodically validate whether stated security controls are implemented correctly, operating as intended, and meet FedRAMP baseline security controls.

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

Privacy controls were engineered into the platform from the initial design phase and will be included at all subsequent development phases. The system owner vets all significant enhancements and changes to the platform prior to the initiation of development efforts. The system owner also documents all significant changes on a Privacy Threshold Analysis to include the Privacy team in analysis of possible additional privacy risks. Finally, the system owner documents the privacy controls every two years through the PIA review process. These privacy controls are then assessed by the Security Authorization Team and the Privacy office.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

The Enterprise ICAM system has the following risks associated with privacy:

- Unauthorized access to personally identifiable information
- Mishandling or misuse of personally identifiable information and,
- Collection of incorrect data.

Risk to data maintained by the Enterprise ICAM System is mitigated by a comprehensive security program over the entire platform and its supporting business processes. A key component of the security program is the continuous monitoring effort which ensures that the security and privacy controls remain in force over-time and that new threats are assessed, and appropriate countermeasures implemented.

The risk of unauthorized access to PII is mitigated through an array of safeguards including: strict access controls, segregation of duties, physical access controls at the hosting facility, data encryption (both in flight and at rest), annual access certifications and network and host-based intrusion detection systems.

The risk of mishandling or misuse of PII is mitigated through a series of requirements for all Enterprise ICAM system administrators:

- both prior to employment and as part of continuous monitoring, ICAM system administrators are subject to background checks
- prior to gaining system access with elevated privileges, system administrators are required to sign a Rules of Behavior which governs their actions and,
- all system administrators participate in annual Privacy training.

Additionally, one of the main purposes of the system itself is to automate the handling of PII so that human interaction with data is reduced thereby decreasing the opportunity for incorrect data to be entered.